REMARKS

The Examiner rejected claims 1-10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565) in view of Perlman et al. (U.S. Patent No. 6,230,266).

Applicants respectfully traverse the §103(a) rejections with the following arguments.

35 U.S.C. §103(a)

The Examiner rejected claims 1-10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565) in view of Perlman et al. (U.S. Patent No. 6,230,266).

Applicants respectfully contend that claims 1 and 6 are not unpatentable over Lewis in view of Perlman, because Lewis in view of Perlman does not teach or suggest each and every feature of claim 1. For example, Lewis in view of Perlman does not teach or suggest: "verifying by the browser the original authentication certificate **using the expired public key of the certifying authority**" (emphasis added) (claim 1), and similar language for claim 6.

The Examiner that Lewis discloses "accepting the transaction by the browser after verification of the original authentication certificate using the expired public key of the certifying authority, and verifying the said SCAC certificate using the new public key of the said certifying authority. (see col. 30, lines 43-50 : When a certificate expires, the certification authority will issue a new certificate and sign it with the old certificates matching private key. The CA will send a new certificate signed with the CA's new private key to the server. The server will validate the certificate for authenticity by first checking to ensure that the new CA certificates public key authenticates the included signature. It will then hash the keys included with the new certificate to verify that the hash value match with the old hash included with the old CA's certificate.)".

In response to the preceding argument by the Examiner, Applicants maintain that there is no disclosure in col. 30, lines 43-50 of Lewis that the original authentication

certificate is verified by using the expired public key of the certifying authority. As the Examiner clearly states, the server hashes the keys included with the new certificate to verify that the hash value matches the old hash included with the old CA's certificate. Applicants maintain that the "old hash" referred to by the Examiner is the "hash of the next certificate key values" (see Lewis, col. 30, lines 37-39) which is the hash of the keys of the new certificate (i.e., "next certificate" means "next new certificate"). Applicants' preceding interpretation of "old hash" must be correct because the only possibility for the hash value of the keys in the new certificate to match the old hash is if the old hash has the hash value of the keys of the new certificate. Thus, the "old hash" is unrelated to the expired public key of the certifying authority. Accordingly, Lewis does not disclose in col. 30, lines 43-50 that the original authentication certificate is verified by using the expired public key of the certifying authority, as required by claims 1 and 6.

In addition, Lewis in view of Perlman does not teach or suggest "presenting the original valid authentication certificate **together with** the said server certifying authority chain certificate, by the server to the browser during the SSL handshake" (emphasis added) (claim 1), and similar language for claim 6. Lewis does not disclose in col. 30, lines 43-50 that the original valid authentication certificate will be included **together with** the new certificate when the USPS CA sends the new certificate to the server, as required by claims 1 and 6..

Based on the preceding arguments, Applicants respectfully maintain that claims 1

and 6 are not unpatentable over Lewis in view of Perlman, and that claims 1and 6 are in condition for allowance. Since claims 2-5 depend from claim 1, Applicants contend that claims 2-5 are likewise in condition for allowance. Since claims 7-10 depend from claim 6, Applicants contend that claims 7-10 are likewise in condition for allowance.

CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below.

Date: 05/24/2004

Jack P. Friedman
Registration No. 44,688

Schmeiser, Olsen & Watts
3 Lear Jet Lane, Suite 201
Latham, New York 12110
(518) 220-1850